Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A system of real time monitoring and control of networked computers, comprising:

a monitoring computer unit capable of being communicatively coupled to a network system; and

a client computer unit capable of being communicatively coupled to the network system, the client computer including a client application that can detect states in the client computer and transmit the detected states to the monitoring computer unit via the network system to permit detection of an unauthorized software program or unauthorized behavior within the client computer unit, wherein the detection of the states includes calculating a maximum base count for entries in a defined registry segment in an internal registry in the client computer unit, and wherein the client application detects states in the client computer by detecting a modification of registry configuration data in the internal registry in the client computer unit.

Claim 2 (original): The system of claim 1 wherein the monitoring computer unit includes an administrator application capable to analyze the transmitted detected states.

Claim 3 (original): The system of claim 2 wherein the administrator application is capable to issue command signal to control the client computer unit in response to a particular detected state in the client computer unit.

Claim 4 (currently amended): A method of real time monitoring and control of networked computers, comprising:

providing a monitoring computer unit and client computer unit both capable of being communicatively coupled to a network system; and

detecting states in the client computer unit and transmitting the detected states to the monitoring computer unit via the network system to permit detection of an unauthorized software program or unauthorized behavior within the client computer unit, wherein the detection of the states includes calculating a maximum base count for entries in a defined registry segment in an internal registry in the client computer unit, and detecting the states in the client computer unit comprises detecting a modification of registry configuration data in the internal registry in the client computer unit.

Claim 5 (new): The system of claim 1, wherein the internal registry comprises a database that is used by an operating system in order to store configuration information.

Claim 6 (new): The system of claim 1, wherein the client application retrieves the registry configuration data and stores the registry configuration data into a memory array,

prior to detecting a modification of the registry configuration data.

Claim 7 (new): The system of claim 1, wherein the client application detects states in the client computer by detecting a modification of internal directory information and file information in the client computer.

Claim 8 (new): The system of claim 7, wherein the client application retrieves the internal directory information and file information and stores the internal directory information and file information into a memory array, prior to detecting a modification of the internal directory information and file information.

Claim 9 (new): The system of claim 1, wherein the internal directory information and file information are required to initiate a third-party application program.

Claim 10 (new): The system of claim 1, wherein the internal directory information and file information are required to initiate the computer unit and the programs for initializing a third-party application program.

Claim 11 (new): The system of claim 1, wherein the client application intercepts messages generated between an operating system and a third-party application program, in order to determine if an action by a user of the client computer is authorized.

Claim 12 (new): The system of claim 11, wherein the client application monitors and intercepts the messages between the operating system and a third-party application program by accessing a memory buffer.

Claim 13 (new): The method of claim 4, wherein the internal registry comprises a database that is used by an operating system in order to store configuration information.

Claim 14 (new): The method of claim 4, further comprising:

analyzing, by the monitoring computer unit, the transmitted detected states that are transmitted by the client computer unit.

Claim 15 (new): The method of claim 4, further comprising:

issuing, by the monitoring computer unit, a command signal to control the client computer unit in response to a particular detected state in the client computer unit.

Claim 16 (new): The method of claim 4, further comprising:

prior to detecting a modification of the registry configuration data, retrieving the registry configuration data, and storing the registry configuration data into a memory array.

Claim 17 (new): The method of claim 4, further comprising:

detecting a modification of internal directory information and file information in the client computer unit.

Claim 18 (new): The method of claim 17, further comprising:

retrieving the internal directory information and file information, and storing the internal directory information and file information into a memory array, prior to detecting a modification of the internal directory information and file information.

Claim 19 (new): The method of claim 4, further comprising:

intercepting messages generated between an operating system and a third-party application program, in order to determine if an action by a user of the client computer unit is authorized

Claim 20 (new): The method of claim 19, wherein the act of intercepting the messages between the operating system and a third-party application program comprises accessing a memory buffer.